Sveučilište Jurja Dobrile u Puli

Fakultet informatike u Puli

JOSIP DŽAJA

BEŽIČNI SUSTAV WI-FI

Završni rad

Pula, 2019.

Sveučilište Jurja Dobrile u Puli

Fakultet informatike u Puli

JOSIP DŽAJA

BEŽIČNI SUSTAV WI-FI

Završni rad

JMBAG: ……..... , redoviti student
Studijski smjer: Informatika

Predmet: Računalne mreže
Znanstveno područje: Društvene znanosti
Znanstveno polje: Informacijske i komunikacijske znanosti
Znanstvena grana: Informacijski sustavi i informatologija

Mentor: Mario Radovan

Pula, 2019.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani _____, kandidat za prvostupnika informatike, smjera _____ ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

_____

U Puli, _____, _____ godine

IZJAVA

o korištenju autorskog djela

Ja, _____ dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj završni rad pod nazivom _____ _____ koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, _____ (datum)

Potpis

_____

SADRŽAJ

UVOD

U današnje vrijeme bilo koji korisnik susreo se sa nekom vrstom uređaja koja koristi bežičnu tehnologiju. To može biti mobilni uređaj, tablet, laptop pa čak i klimatizacijski uređaji. S obzirom da se danas velika većina populacije koristi pametnim telefonima, često nam je potreban Internet. Tako se, u posljednje vrijeme, sve više spominje pojam Wi-Fi. Wi-Fi nam omogućuje povezivanje na Internet te „surfanje“ u svrhu pretraživanja raznih podataka, pregled vijesti, temperature te ponajviše razmjene poruka i poziva sa ostalim korisnicima.

Sam Wi-Fi nam to uvelike olakšava. Uz povećanu mobilnost i jednostavnost korištenja, kroz nekoliko klikova možemo pronaći što nas zanima, di se nalazimo ili pak nazvati nekoga. No često korisnici nisu upućeni u to da Wi-Fi nosi i svoje posljedice. Tako se može dogoditi da korisnik, spojen na javnu Wi-Fi mrežu, ide pregledavati neke osobne podatke, stanje svog bankovnog računa preko posebnih aplikacija, pregledavanje osobnog ili poslobnog e-maila za koje je svima bitno da ostanu privatni te da ne dođu u opasnost da im se ti isti podaci ne otuđe od potencijalne krađe. Često se u medijima može naići na članke vezane uz tzv. hakiranje podataka raznim metodama u svrhu otuđenja podataka, pa čak i krađe novca sa bankovnih računa.

Sigurnost je danas najbitnija stvar kada je u pitanju spajanje na određene Wi-Fi mreže i vrlo bitna stvar samih korisnika takvih mreža. Tako su Wi-Fi mreže danas jedne od najranjivijih vrsta mreža jer se zbog načina odašiljanja podataka te same infrastrukture Wi-Fi mreže vrlo lako mogu presresti informacije kojim korisnik rukuje dok je spojen na neku Wi-Fi mrežu.

Ono što će biti obuhvaćeno u ovom radu je način funkcioniranja sustava Wi-Fi, kada i na koji način je razvijen, potrebne komponente, način postavljanja Wi-Fi mreže te sama sigurnost i kako ju unaprijediti.

1. ŠTO JE WI-FI?

Naziv Wi-Fi označava jedan skup mreža koje se međusobno razlikuju u raznim elementima i koje su definirane raznim varijantama standarda 802.11. Wi-Fi je zaštitni znak (trademark) udruženja zvanog Wi-Fi Alliance. Ono okuplja oko 300 tvrtki koje proizvode opremu za bežične lokalne mreže (wireless LAN – WLAN). To udruženje izdaje certifikate koji potvrđuju da li neki proizvod iz područja bežičnih lokalnih mreža udovoljava zahtjevima standarda 802.11. Bitno je naglasiti da proizvodi mogu udovoljavati zahtjevima tog standarda bez da imaju certifikat Wi-Fi Alliance udruženja[1]. Wi-Fi se prvi put pojavljuje 1991. godine kada ga je izumila NCR korporacija/AT&T u Nieuwegeinu, Nizozemska. Prva napravljena mreža zvala se WaveLAN i radila je na brzinama od 1 do 2 Mbit/s. Najzaslužnijim za stvaranje Wi-Fi-ja smatra se Vic Hayes kada su on i njegov tim osimislili standarde za Wi-Fi pod nazivom IEEE 802.11, te danas postoje 802.11a, 802.11, i 802.11g, 802.11n te mnogi ostali[2]. O navedenim standardima bit će više riječi kasnije.

Wi-Fi mreža je bežična lokalna mreža namijenjena uporabi u lokalnim prostorima kao što su poslovne zgrade ili sjedište neke institucije koja obuhvaća više zgrada na jednom mjestu. Bežične mreže odlikuje sljedeće: omogućuju bežično povezivanje računala ili nekog drugog uređaja na mrežu i pružaju dobru, ali ne tako veliku, mobilnost računala. Bežične veze kao takve vrlo često smanjuju troškove vezivanja na mrežu, jer se npr. kod mobilnih uređaja spajanje na mrežu mobilnog operatera naplaćuje, a u određenim slučajevima spajanje na mrežu bežičnom vezom je nužno tamo gdje nije moguće ili dopušteno postavljati žice. Naime, mobilnost kod bežičnih mreža nije velika te iznosi otprilike 100 metara, a u nekim slučajevima i manje od toga. To u nekim slučajevima može biti pogodno jer omogućava komuniciranje u lokalnoj mreži ili preko interneta sa mjesta na koje se obično ne postavljaju žice kao što su dvorišta kuća ili parkovi.

Za spajanje na Wi-Fi mrežu potrebno je imati mrežni adapter za standard 802.11 za Wi-Fi mrežu. Takav mrežni adapter adapter uključuje transiver (odašiljač i prijamnik) za bežične, odnosno elektromagnetske, signale. Prijenosna računala, s druge strane, mogu

[1] M. Radovan, *Računalne mreže (1),* Rijeka, Digital point tiskara, 2010., str. 273. [02. srpnja 2019.]
[2] Spahić, A. (2011). *Bežične Wi-Fi Računarske mreže i sigurnost Wi-Fi mreža*, seminarski rad. Zenica : Pedagoški Fakultet [24. srpnja 2019.]

imati ugrađene adaptere za Wi-Fi mreže. U slučaju da računalo nema ugrađen potrebni adapter, taj adapter se može ugraditi ili se može priključiti na neki od USB portova računala.

Osnovna struktura Wi-Fi mreže čine *točke pristup*a i *žičani distribucijski sustav*.

Točke pristupa (eng. *access point – AP)* su točke na koje se računala povezuju bežičnim putem. Točke pristupa još se nazivaju vrućim točkama (eng. *hot spots*). Nakon povezivanja na točku pristupa računalu se omogućuje komuniciranje sa mrežom bežičnim putem sa drugim računalima koja su vezana na istu točku pristupa. Točke pristupa su međusobno povezane preko distribucijskog sustava koji omogućava komunikaciju između računala koje su vezane na različite točke pristupa.

Distribucijski sustav je obično lokalnih razmjera što znači da to može biti jedna mreža tipa Ethernet te se zbog toga Wi-Fi mreža ponekad naziva bežičnim Ethernetom. Povezanost distribucijskog sustava na Internet omogućava računalima bežični pristup Internetu. Bitno je spomenuti da bežični LAN nije primjeren naziv jer se, iako se računala povezuju na LAN bežičnim putem, njegov distribucijski sustav je obično neki žičani LAN[3].

1.1. IEEE 802.11 standardi

IEEE (*eng. Institute of Electrical and Electronics Engineers*) je institut koji je 1997. godine razvio standarde koje danas poznajemo kada je u pitanju bežična mreža. Od svih razvijenih standarda, najznačajniji su 802.11 standardi koje koristi Wi-Fi, a trenutno su najviše u upotrebi. Svi navedeni standardi koriste Ethernet protokol te se razlikuju po brzinama prijenosa te broju kanala.

1.1.1. 802.11a

Ovaj standard, teoretski, raspolaže brzinama od 54 Mbps ali najčešće ona iznosi između 6 i 24 Mbps. Ovaj standard radi na području frekvencije od 5GHz. Naime, to područje frekvencije se puno manje koristi nego u ostalim standardima pa se zbog toga događa puno manje međusobnih smetnji (tzv. interferencija) između signala različitih bežičnih

[3] ibidem, str. 274.

mreža. Problem koji se pojavljuje kod tog područja frekvencije je taj da je u tom području uvelike povećana apsorpcija bežičnih signala što dovodi do ograničavanja mogućnosti bežičnog prijenosa podataka.

1.1.2. 802.11b

Ovaj standard je predstavljen 1999. godine i radi na frekvenciji od 2,45GHz. Brzine prijenosa podataka iznose 11 Mbps pomoću Complementary Code Keying (CCK) tehnologije koji je bio vrlo ekonomična nadogradnja postojećih 802.11 čipova. To je omogućilo masovnu proizvodnju jeftinih i dovoljno brzih uređaja te je time započeo proces popularizacije 802.11X tehnologije. Brzine koje je moguće postići su na oko 6 Mbps. Ovaj standard koristi maksimalno 14 kanala (što ovisi o regiji u kojoj se koristi pa tako SAD ima 11, a Europa 13 kanala) od kojih se 3 ne preklapa. Standard 802.11b+ donesen je od strane proizvođača Texas Instruments i njihovog ACX100 čipa. On naime donosi brzine od 22 do 44 Mbps te koristi Packet Binary Convolution Coding (PBCC) modulacijsku tehnologiju. Također, povećana je sigurnost, a realne brzine koje ovaj standard može postići su oko 10 Mbps

1.1.3. 802.11g

Prijedlog za standard 802.11g donesen je 2003. godine i ovaj je standard danas poprilično popularan te defakto sinonim za Wi-Fi. Donosi brzine transfera podataka od 54 Mbps te koristi Orthogonal Frequency-Division Multiplexing (OFDM) modulacijsku tehnologiju za brzine prijenosa od 6, 9, 12, 18, 24, 36, 48 i 56 Mbit/s. Za brzine od 5,5 i 11 Mbps koristi CCK modulaciju (kao 802.11b) te Differential Binary/Quadrature Phase-shift Keying + Direct-Sequence Speed Spectrum (DBPKS/DQPKS+DSSS) za 1 i 2 Mbit/s. Maksimalna brzina koju postiže je oko 22 Mbps, a koristi iste kanale kao i 802.11b[4].

[4] Spahić, A. (2011). *Bežične Wi-Fi Računarske mreže i sigurnost Wi-Fi mreža*, seminarski rad. Zenica : Pedagoški Fakultet [24. srpnja 2019.]

1.1.4. 802.11n

Ovaj standard, predstavljen 2009. godine, polako je počeo sa usvajanjem. 802.11n radi na frekvencijama od 2,4GHz i 5GHz te podržava višekanalno korištenje. Svaki kanal nudi brzinu prijenosa podataka od 54 Mbps, pa sve do maksimalne brzine prijenosa podataka od 600 Mbps. Ovaj standard uveo je tehnologiju pod naziv MIMO (Multiple-Input Multiple-Output). Ova tehnologija koristi više antena za koherentno rješavanje više informacija nego što je moguće pomoću jedne antene. Jedan od načina da to omogući jest pomoću prostornog multipleksiranja (eng. Spatial Division Multiplexing – SDM) koje prostorno multipleksira više neovisnih podatkovnih tokova koji se istovremeno prenose unutar jednog spektralnog kanala propusne širine. MIMO SDM može značajno povećati propusnost podataka jer se povećava broj riješenih tokova prostornih podataka te to omogućuje skoro 10 puta veće brzine od brzina koje je nudio standard 802.11g.

1.2. Prednosti i nedostatci

Wi-Fi, kao način bežičnog povezivanja, nudi razne pogodnosti, pretraživanje podataka na Internetu te pregledavanje osobnih podataka itd. Ali, koliko god to svima koristilo, Wi-Fi ima svoje prednosti i nedostatke.

1.2.1. Prednosti

1) Učinkovitost – prijenos informacija je brz i praktičan. Vrlo dobar za razne tvrtke ili korporacije jer omogućava zaposlenicima pregled podataka bilo gdje u tvrtci, a samim time i povećava produktivnosti na radnom mjestu.
2) Fleksibilnost – krajnji korisnici nisu ograničeni na jednu fizičku lokaciju prilikom povezivanja na bežičnu mrežu.
3) Isplativost – bežične mreže i njihovo postavljanje su relativno jeftine za instalaciju u nekoj tvrtci ili korporaciji te nudi veće mogućnosti pri odabiru računalne opreme.

4) Pristupačnost – Wi-Fi je danas izarazito popularan u javnim okruženjima kao npr. kafići, knjižnice, hoteli ili restorani. Javno dostupan Wi-Fi olakšava povezivanje na Internet[5].

1.2.2. Nedostatci

1) Napadi virusa / hakiranje uređaja – ovisno o sigurnosti uređaja s kojim se spaja na neku mrežu, postoji vjerojatnost da drugi ljudi napadnu uređaj (pošalju virus, „preuzmu“ naš uređaj..) dok je spojen na određenu Wi-Fi mrežu.
2) Krađa podataka – nešifrirana vrsta podataka, kao npr. provjeravanje e-maila, može biti preuzeta od strane hakera dok se prenosi između Wi-Fi mreže i uređaja ili dok se prenosi na mreži.
3) Krađa računa registriranih na internetskim stranicama – podaci za prijavi na neki internetski račun poput Google, Youtube, Facebook i drugih mogu biti ukradeni od strane drugih osoba na mreži ako ta mreža nije kriptirana[6].
4) Performanse / brzina – brzine prijenosa podataka u raznim kafićima, restoranima ili hotelima nisu izrazito brze što otežava rad i „surfanje“ Internetom[7].

[5] Solvere One Blog [online], *The Pros and Cons of Wi-Fi*, Washington, D.C. Dostupno na: https://www.solvereone.com/pages/the-pros-and-cons-of-wi-fi/ [02. srpnja 2019.]
[6] Arun (2013.), *What is Wi-Fi* [online], Scribd, Dostupno na: https://www.scribd.com/document/192846073/Wifi [03. srpnja 2019.]
[7] Krishnasamy, T. (2017.), *What are the advantages and disadvantages of WiFi?*, Quora. Dostupno na: https://www.quora.com/What-are-the-advantages-and-disadvantages-of-WiFi [03. srpnja 2019.]

2. KOMPONENTE WI-FI-ja

Ključne komponente neke bežične mreže uključuju modem, mrežnu karticu, usmjerivač (router), pristupne točke, antene i repetitore.

2.1. Modem

Modem je uređaj za hardversko umrežavanje koji pretvara podatke u signal tako da se mogu lako slati i primati putem telefonske linije, kabela ili satelitske veze. Prije su modemi radili preko analogne telefonske linije koja je u to vrijeme bila vrlo popularna za povezivanje na Internet, te kod njih modem pretvara podatke između analognih i digitalnih formata u realnom vremenu za dvosmjernu mrežnu komunikaciju. U slučaju popularnih digitalnih modema velike brzine, signal je mnogo jednostavniji i ne zahtjeva analogno-digitalno pretvaranje[8].

Slika 1. Modem

Izvor: https://www.123rf.com/photo_9043027_dsl-modem.html

2.2. Mrežna kartica

Mrežne kartice od velike su važnosti te su potrebne za svaki uređaj na bežičnoj mreži. To je dio koji se brine za komunikaciju računala preko računalne mreže odnosno za priključivanje računala ili nekog drugog uređaja na lokalnu mrežu. Svaki noviji uređaj

[8] Mitchell, B. (2019.), *What is a modem in Computer Networking?*, Lifewire. Dostupno na: https://www.lifewire.com/what-is-a-modem-817861 [16. srpnja 2019.]

poput pametnih telefona, prijenosnih računala, tableta i ostalih imaju mogućnost bežičnog povezivanja kao ugrađenu značajku svojih sustava.

Slika 2. Mrežna kartica

Izvor: https://www.links.hr/hr/mrezne-kartice-i-adapteri-053503

2.3. Usmjerivač (router)

Usmjerivač je srce neke bežične mreže. On funkcionira usporedivo kao i tradiocionalni usmjerivači za žičane Ethernet mreže. Kako bi se uspostavila bežična mreža u kući ili uredu, potreban je bežični usmjerivač. Trenutni standard za bežične usmjerivače je 802.11ac koji pruža vrlo dobru reprodukciju video zapisa ili igranje online video igara. Stariji usmjerivači su sporiji, ali će obavljati posao, pa se pri izboru usmjerivača gleda koja će mu svrha biti i za što će se koristiti.

Slika 3. Bežični usmjerivač (router)

Izvor: https://www.links.hr/hr/routeri-053524

2.4. Točka pristupa (access point)

Točka pristupa se koristi kako bi se dopustilo bežičnoj mreži da se spoji na već postojeću mrežu. Drugim riječima, točka pristupa nam može pomoći u slučaju ako u nekom dijelu kuće, poslovnog prostora ili zgrade imamo slabu mrežu i otežan pristup spajanja na Wi-Fi. Postavljanjem točke pristupa na to mjesto i spajanjem na mrežu koju koristimo, olakšavamo spajanje na mrežu na prostoru u kojem to ili nije bilo moguće ili vrlo otežano.

Slika 4. Pristupna točka

Izvor: https://www.links.hr/hr/access-point-053509

2.5. Antene

Wi-Fi bežično umrežavanja funkcionira tako da šalje radio valove na određenim frekvencijama gdje ih slušni uređaji mogu primati. Potrebni radijski odašiljači i prijemnici ugrađeni su u opremu koja podržava Wi-Fi kao što su usmjerivači, pametni telefoni, prijenosna računala i ostali. Antene su također ključne komponente ovih radiokomunikacijskih uređaja zbog toga što prikupljaju dolazne signale ili zračenje odlaznih Wi-Fi signala. Neke Wi-Fi antene, osobito na usmjerivačima, mogu se ugraditi izvana, dok su druge ugrađene unutar hardverskog kućišta nekog uređaja.

Slika 5. Wi-Fi antena

Izvor: https://www.instar-informatika.hr/antene/

2.6. Repetitor

Wi-Fi repetitor ili ekstender koristi se kako bi se proširilo područje pokrivanja Wi-Fi mreže. Repetitor radi na način da, nakon što primi postojeće Wi-Fi signale, pojača signal i prenosi takav pojačani signal. Pomoću repetitora se može unčikovito i na jednostavan način udvostručiti područje pokrivanja Wi-Fi mreže dosežući daleke kuteve kuće, ureda itd[9]. Kod postavljanja reptitora, on mora biti izravno povezan sa usmjerivačem. Kako bi se postigli najbolji rezultati, tvrtka Microsoft predlaže postavljanje repetitora na pola puta između usmjerivača i uređaja kojim se spajamo na Wi-Fi mrežu. U slučaju da u području kuće ili ureda uređaj kojim se spajamo na Wi-Fi mrežu uopće ne prima bežični signal, web stranica Wireless Nets, Ltd. predlaže postavljanje repetitora na točku između pokrivene i nepokrivene površine.

Jedan od potecijalnih nedostatak repetitora jest taj da koristi propusni kapacitet mreže, što je zapravo njegov propusni opseg. Proces primanja i ponovnog slanja podatkovnih okvira zapravo udvostručuje količinu korištenih okvira, što znači da je kapacitet prijenosa prepolovljen. To može utjecati na ukupnu učinkovitost i brzinu same mreže na koju se osoba spaja svojim uređajem. Ako se koristi repetitor koji nije pružio isti dobavljač koji

[9] Karan, T., Aggarwal, A., Masih, D., (2018.), *Wi-Fi Technology* [online], Scribd. Dostupno na: https://www.scribd.com/document/373130860/WiFi-Technology-Bss [03. srpnja 2019.]

osigurava točku pristupa na koju se osoba spaja, također postoji mogućnost da će repetitor slabije raditi i signal će biti slab[10].

2.7. Domet Wi-Fi-ja

Jedna od najvećih mana bežične mreže Wi-Fi je njen domet. Jako mali domet ograničava rad, zahtjeva nadogradnju što iziskuje dodatne troškove nekog kućanstva ili tvrtke. Naime, kako bi se povećao domet potrebno je u cijelu konfiguraciju ugraditi dodatne točke pristupa. Točke pristupa trenutno variraju u cijenama ali ako želimo nadograditi sustav, želimo da to bude što bolje i što pouzdanije.

Kod manjih kućanstava, obično je bežični usmjerivač (ruter) dovoljan kako bi se pokrilo cijelo kućanstvo. Bitno je naglasiti da sam domet signala neke točke pristupa ovisi od uređaja do uređaja. Neki od faktora koji utječu na domet neke točke pristupa uključuju

- Određeni 802.11 standard
- Jačina odašiljača koji uređaj ima
- Priroda fizičkih prepreka i/ili radio smetnji u okolnom području

Postoji opće pravilo da u kućnom umrežavanju da Wi-Fi usmjerivači koji rade na frekvenciji od 2,4 GHz dopiru do 46 metara u zatvorenom prostoru te 92 metra na otvorenom. Stariji usmjerivači, koji su radili na standardu 802.11a te frekvencijama od 5 GHz, imali su domet od otprilike jednu trećinu tih udaljenosti. Noviji usmjerivači, koji rade na standardima 802.11n i 802.11ac te frekvencijama od 2,4 GHz te 5 GHz, razlikuju se u dometu na sličan način. U manjim kućanstvima koja koriste mikrovalne pećnice, bežične telefone i ostalu opremu također negativno utječu na domet Wi-Fi mreže. Budući da se radio uređaji sa frekvencijama od 2,4 GHz obično koriste u „gadgetima“ za potrošače, ti standardi Wi-Fi veza su podložniji smetnjama unutar stambenih zgrada. Također, udaljenost na kojoj je nekome omogućeno povezivanje na Wi-Fi mrežu razlikuje se ovisno o tome kako je orijentirana antena mrežnog usmjerivača. Za korisnike pametnih telefona, to je vrlo lako provjeriti jer samim zakretanjem svog uređaja mogu vidjet kako se signal

[10] Joseph, C., *What does a Wi-Fi repeater do?*, Small Business – Chron.com. Dostupno na: https://smallbusiness.chron.com/wifi-repeater-do-31941.html [09. srpnja 2019.]

Wi-Fi mreže povećava ili smanjuje. Isto tako, neke pristupne točke koriste usmjerene antene koje omogućuju dulji doseg u područjima na koje je usmjerena antena, ali kraći doseg prema drugim područjima[11].

3. SIGURNOST WI-FI MREŽE

Najveća mana svih Wi-Fi mreža danas je sigurnost. O sigurnosti ovise svi podaci koje neka osoba pregledava sa svog uređaja i ako je sigurnost loša, postoji mogućnost da osobi budu otuđeni podaci. Vrlo je bitno osigurati bilo koju mrežu, pogotovo mreže koje se koriste u kućanstvima jer kroz takve mreže svi ukućani pregledavaju svoje bankovne račune, e-mailove i razne druge stvari koji mogu biti otuđene od strane nekih trećih osoba. Zaštitom takvih mreža određenim metodama sigurnost se uvelika povećava. Postoje razne metode osiguravanja Wi-Fi mreže o čemu će biti riječ u nastavku.

Od kasnih 1990-ih godina, sigurnosni Wi-Fi protokoli prošli su razne nadogradnje, gdje stariji protokoli jednostavno više nisu bili pouzdani te se okrenula pažnja na novije protokole.

3.1. Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) je predstavljen kao prvi Wi-Fi sigurnosni protokol na svijetu. WEP je potvrđen kao Wi-Fi sigurnosni protokol u rujnu 1999. godine. Prve razvijene verzije WEP-a nisu bile osobito jake i pouzdane, čak ni za vrijeme kada su objavljene, jer su američka ograničenja za izvoz različitih kriptografskih tehnologija dovela do toga da ograničavaju svoje uređaje na samo 64-bitno šifriranje. Nakon ukidanja ograničenja, šifriranje je povećano na 128-bitno. Iako se uvelo 256-bitno WEP šifriranje, 128-bitni ostaje jedna od najčešćih implementacija. Unatoč ispravljanju protokola i povećanoj veličini ključa, kroz neko vrijeme otkrilo se da WEP standard ima brojne

[11] Mitchell, B. (2019.), *The range of typical Wi-Fi Network* [online], Lifewire. Dostupno na: https://www.lifewire.com/range-of-typical-wifi-network-816564 [04. srpnja 2019.]

sigurnosne propuste. Unatoč povećanju snage rada računala, postalo je sve lakše i lakše iskoristit te nedostatke. Kada je već bilo sigurno pričati o WEP sigurnosnom protokolu, FBI je 2005. godine javno demonstrirao (u nastojanju da poveća svijest o slabostima WEP-a) kako su u samo nekoliko minuta probili WEP-ove lozinke koristeći besplatno dostupne softvere. Bez obzira na razna poboljšanja, radnim okolnostima i drugim pokušajima da se WEP sustav učvrsti, on i dalje ostaje vrlo ranjiv. Sustave koji se oslanjaju na WEP sigurnosni standard potrebno je nadograditi ili, ako sigurnosne nadogradnje nisu opcija, zamijeniti. Wi-Fi Alliance službeno je povukao WEP sigurnosni standard 2004. godine.

3.2. Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA) bio je direktan odgovor i zamjena za Wi-Fi Alliance sve očitijim i lošijim WEP sigurnosnom standardu. WPA je službeno usvojen 2003. godine, godinu dana prije službenog umirovljenja WEP sigurnosnog standarda. Najčešća WPA konfiguracija je WPA-PSK (Pre-Shared Key). Ključevi koje koristi WPA sigurnosni standard su 256-bitni, što je uvelike značajnije od 64-bitnih i 128-bitnih ključeva koje su korišteni u WEP sustavu. Neke od značajnijih promjena koje su implementirane u WPA sigurnosni standard uključivale su provjeru integriteta poruka. Tako se moglo utvrditi je li napadač zarobio ili promijenio pakete koji su prošli između točke pristupa i klijenta. Također, koristio se i TKIP (Temporal Key Integrity Protocol). TKIP koristi sustav ključa po paketu koji je bio radikalno sigurniji od sustava fiksnih ključeva koji koristi WEP. TKIP standard za enkripciju kasnije je zamijenjen Advanced Encription Standard-om (AES).

Unatoč tome što je WPA značajno poboljšanje naspram WEP sigurnosnog standarda, duh WEP-a je proganjao WPA. TKIP, ključna i najbitnija komponenta WPA, dizajnirana je tako da se može lako izvesti kroz nadogradnju firmware-a na već postojeće uređaje koje koriste WEP. Kao takav, morao je reciklirati određene elemente koji se koriste u WEP sustavu i koji su u konačnici također iskorišteni. WPA, kao i njegov prethodnik WEP, je pokazan kroz javne demonstracije kao slab i lako probijen sigurnosni standard. Zanimljivo je to da proces kroz koji se probija WPA standard nije izravan napad na WPA protokol (iako su takvi napadi uspješno demonstrirani), nego napad na dodatni sustav koji je

uveden zajedno sa WPA-om – Wi-Fi Protected Setup (WPS) – koji je dizajniran kako bi se olakšalo povezivanje uređaja sa modernim točkama pristupa.

3.3. Wi-Fi Protected Access II (WPA2)

WPA je od 2006. godine službeno zamijenjen WPA2 sigurnosnim standardom. Kao jedna od najznačajnijih promjena između WPA i WPA2 je ta da se obavezno morao koristiti AES algoritam te se uz to uveo i CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) kao zamijena za TKIP. Međutim, TKIP se još uvijek čuva u WPA2 kao zamjenski sustav i za interoperabillnost WPA sigurnosnog standarda. Trenutno je primarna sigurnosna ranjivost stvarnog WPA2 sustava nejasna i od napadača zahtijeva da već ima pristup zaštićenoj Wi-Fi mreži kako bi dobio pristup određenim ključevima, a zatim nastavio napad na druge uređaje. Kao takve, sigurnosne implikacije poznatih WPA2 ranjivosti gotovo su u potpunosti ograničene na mreže na razini poduzeća i zaslužuju malo ili nimalo praktičnog razmatranja u pogledu sigurnosti kućne mreže. Nažalost, ista ranjivost koja je najveći problem u WPA oklopu – vektor napada kroz Wi-Fi Protected Setup (WPS) – ostaje u modernim točkama pristupa koje koriste WPA2 standard. Iako provala u WPA / WPA2 zaštićenu mrežu koja koristi ovu ranjivost zahtijeva od 2 do 14 sati trajnog napora s modernim računalom, to je i dalje legitimna sigurnosna briga. WPS bi trebao biti omogućen, i ako je moguće, firmware pristupne točke trebao bi biti prebačen na distribuciju koja ne podržava čak ni WPS tako da je vektor napada potpuno uklonjen[12].

Trenutno, najpoznatija sigurnosna metoda korištena danas (i koju bi svi trebali koristiti na svojim Wi-Fi mrežama) je WPA2 + AES. Ljestvica koja prikazuje najsigurnije standarde, poredane od najsigurnijih do najnesigurnijih, izgleda ovako:

1) WPA2 + AES
2) WPA + AES
3) WPA + TKIP/AES (TKIP se koristi kao posljedična metoda)

[12] Fitzpatrick, J. (2017.), *The Difference between WEP, WPA and WPA2 Wi-Fi passwords*, How-To-Geek. Dostupno na: https://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/ [09. srpnja 2019.]

4) WPA + TKIP
5) WEP
6) Otvorena mreža (nema nikakve sigurnosti)

Svrha WPA i WPA2 sigurnosnih standarda je da osiguraju Wi-Fi mrežu od neovlaštenog pristupa. Ako osoba ostavi usmjerivač bez sigurnosti, svatko ima mogućnost ukrasti propusnost, izvesti nezakonite radnje izvan Wi-Fi veze i naziva, nadzirati web aktivnosti i jednostavno instalirati zlonamjerne aplikacije u Wi-Fi mrežu.

S obzirom da usmjerivači danas podržavaju razne standarde poput navedenih (WEP, WPA, WPA2), WPA2 se preporučuje najviše u odnosu na WPA. Vjerojatno je jedina mana WPA2 standarda ta kolika je procesorska snaga potrebna za zaštitu neke Wi-Fi mreže. To znači da je potreban snažniji hardver kako bi se izbjegle niže performanse mreže. Ovo se pitanje odnosi na starije točke pristupa koje su implementirane prije WPA2 standarda i podržavaju samo WPA2 putem nadogradnje firmware-a. Većina trenutnih točaka pristupa isporučena je s sposobnijim hardverom. Izrazito se preporuča korištenje WPA2 ako je to moguće, a korištenje WPA standarda samo ako ne postoji mogućnost da pristupna točka ne podržava WPA2 sigurnosni standard. Korištenje WPA je također mogućnost kada točka pristupa redovito doživljava visoka opterećenja i brzina mreže trpi zbog korištenja WPA2. Kada je sigurnost mreže prioritet, tada povratak nije opcija već je potrebno ozbiljno razmotriti dobivanje boljih točaka pristupa. WEP se mora koristiti ako ne postoji mogućnost korištenja bilo kojeg od WPA standarda.

Kod osiguravanja mreže potrebno je koristiti što različitiji skup znakova (korištenje malih i velikih slova, raznih znakova i brojeva). Hakeri su obično zainteresirani za lakše mete koje mogu probiti, te ako ne mogu probiti lozinku u roku od nekoliko minuta, vrlo je vjerojatno da će odustati i tražiti ranjiviju mrežu[13].

[13] Netspot, *Wi-Fi encryption and security*, Netspotapp. Dostupno na: https://www.netspotapp.com/wifi-encryption-and-security.html [09. srpnja 2019.]

4. POSTAVLJANJE WI-FI MREŽE

U nastavku rada biti će objašnjeno kako se i na koji način postavlja Wi-Fi mreža. Kada je u pitanju postavljanje opreme te spajanje svih komponenti u jednu cijelinu, nekima će se to činiti kao težak zadatak. Naime, to uopće nije težak zadatak te cijeli proces traje otprilike 20 minuta. Ono što osoba treba kako bi postavila mrežu i ostvarila konekciju je: bežični usmjerivač (ruter), prijenosno ili stolno računalo (ili bilo koji drugi uređaj koji ima mogućnost spajanja na mrežu), modem te 2 Ethernet kabela. Cijeli proces bit će objašnjen kroz jasne i razumljive korake.

4.1. Pronalaženje pravog mjesta za usmjerivač

Usmjerivač ili ruter je najbolje staviti na neku središnju lokaciju kućanstva gdje nema nikakvih prepreka koje mogu uzrokovati bežične smetnje, poput prozora, zidova pa čak i mikrovalne pećnice.

4.2. Isključivanje modema

Potrebno je ugasiti DSL (Digital subscriber line) modem ili isključiti kabel iz pružatelja internetskih usluga (eng. ISP – Internet service provider) prije nego se počne spajati potreba oprema.

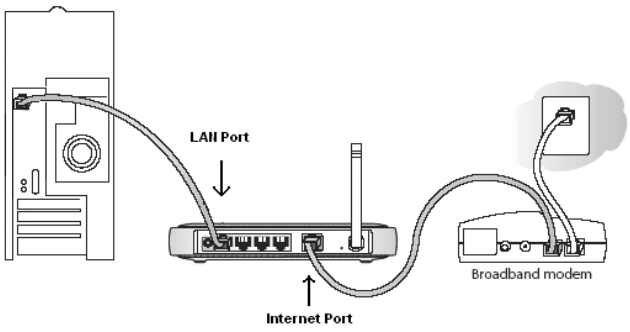
4.3. Spajanje usmjerivača sa modemom

Uključite jedan kraj Ethernet kabela (koji obično dolazi sa usmjerivačem) u usmjerivačev WAN (Wide Area Network) otvor, a drugi kraj Ethernet kabela u modem.

4.4. Povezivanje stolnog/prijenosnog računala sa usmjerivačem

Jedan kraj Ethernet kabela potrebno je uključiti u usmjerivač, dok se drugi kraj kabela uključuje u stolno/prijenosno računalo odnosno u njegov LAN (Local Area Network) otvor. Ovaj korak je samo privremen dok se ne postave sve potrebne opcije kako bi se ostvarila Wi-Fi mreža.

Slika 6. Proces povezivanja usmjerivača, modema i računala



Izvor: https://kb.netgear.com/119/How-to-configure-your-NETGEAR-router-for-cable-internet-connection-with-Smart-Wizard

4.5. Uključivanje modema, usmjerivača i računala

Ovi uređaji se pale navedenim redosljedom. Modem se uključuje u struju, a usmjerivač ima svoj zaseban gumb kojim se pali (također treba biti uključen u struju).

4.6. Namještanje postavki na web stranici usmjerivača

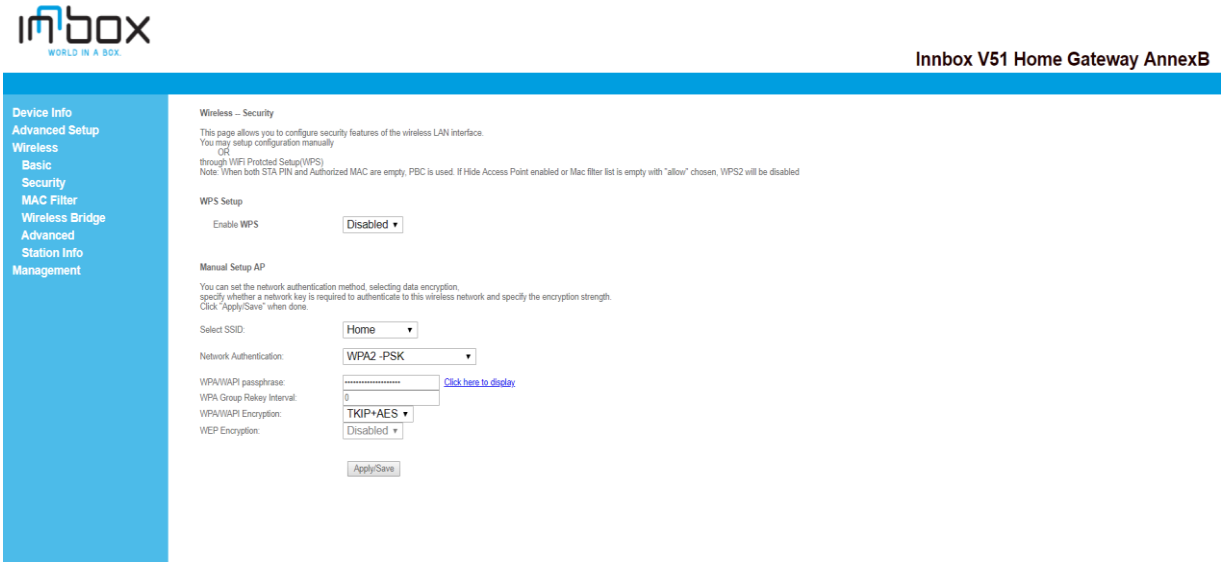
U ovom koraku postavljaju se sve opcije potrebne za ostvarivanje Wi-Fi mreže. Postoje razne opcije, no osim SSID (Service Set Identifier) odnosno naziva mreže i pristupnog ključa (zaporke), ne bi trebalo mijenjati. U slučaju da nešto nije u redu, potrebno je nazvati pružatelja internetskih usluga te razgovarati sa njihovim zaposlenicima kako bi se problem otklonio.

4.7. Dodavanje WPA2 sigurnosnog protokola

Ovaj korak je nužan. Kako bi se povećala sigurnost i spriječila neovlaštena krađa podataka od strane neke treće osobe, ovo je izrazito bitan korak. Ovaj korak moguće je pronaći u odjeljku o sigurnosti bežične mreže, gdje se odabire određena vrsta šifriranja koja će se koristiti te zatim unosi zaporka koja mora imati najmanje 8 znakova. Što je zaporka složenija, smanjuju se šanse osobi koja želi hakirati mrežu da napravi neovlašten

pristup mreži. WPA2 je trenutno najnoviji i najsigurniji protokol šifriranja mreže, uvelike sigurniji od WEP-a. U slučaju da osoba posjeduje stariji bežični usmjerivač na bilo kojem od uređaja koji se spajaju na Wi-Fi mrežu, potrebno je koristiti WPA ili WPA/WPA2 u kombiniranom načinu rada. Trenutno najjača vrsta šifriranja koja je dostupna jest WPA2-AES, no može se koristiti WPA2-PSK (također vrlo sigurna vrsta šifriranja).

Slika 7. Pregled postavki bežične mreže



Izvor: http://192.168.1.1/

Na slici 7. vidimo postavke Wi-Fi mreže koju koristim kod kuće. Kao provjeru autentičnosti mreže koristim WPA2-PSK s obzirom da se radi o maloj kućnoj mreži koju ne koristi puno osoba. Način enkripcije je TKIP-AES jer dopušta maksimalnu kompatibilnost sa bilo kojom vrstom uređaja (bilo koje starosti) koja ima mogućnost spajanja na Wi-Fi mrežu.

4.8. Opcionalno: Promijena bežičnog kanala mreže

U slučaju da se osoba nalazi na mjestu sa puno drugih bežičnih mreža, smetnje se mogu smanjiti promijenom kanala bežične mreže usmjerivača na onaj koji manje koriste druge mreže. Wi-Fi analyzer aplikacija za pametne telefone se može koristiti kako bi se provjerilo

koji kanali na određenom području imaju najmanje gužve (obično su to kanali 1, 6 ili 11 budući da se ne preklapaju).

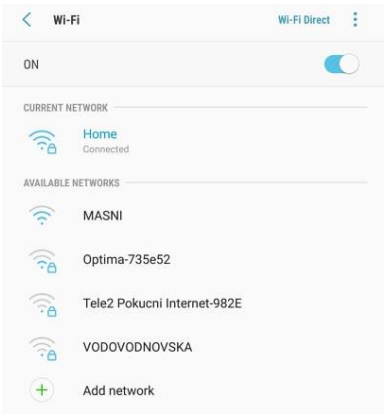
4.9. Postavljanje bežičnog adaptera na računalo

Nakon što korisnik spremi postavke koje je mijenjao na svom usmjerivaču, može isključiti kabel koji povezuje računalo s usmjerivačem. U nekim slučajevima postoji mogućnost da uređaj s kojim se spajamo na Wi-Fi mrežu neće imati instalirane upravljačke programe te bi ih trebalo instalirati pomoću CD-a koji se dobije uz usmjerivač.

4.10. Spajanje na mrežu

Zadnji korak je spajanje na mrežu pomoću uređaja s kojim to želimo. Kada korisnik otvori opciju za Wi-Fi na svom uređaju, pokazat će mu se mreža koju je postavio te unošenjem lozinke koja je postavljena ostvaruje se veza sa tom Wi-Fi mrežom[14].

Slika 8. Ponuđene Wi-Fi mreže na pametnom telefonu



Na Slici 8. vidimo razne Wi-Fi mreže na koje se mogu spojiti svojim mobilnim uređajem te kućna mreža (Home) na koju sam spojen.

[14] Pinola, M. (2019.), *How To Set Up Your Home Wi-Fi Network*, Lifewire. Dostupno na: https://www.lifewire.com/how-to-set-up-your-home-wi-fi-network-2378223 [15. srpnja 2019.]

5. BUDUĆNOST WI-FI-ja

Bežična tehnologija je trenutno u nevjerovatnom i jako brzom razvitku. Način korištenja Interneta je u potpunosti promijenio živote i način poslovanja milijardi ljudi širom svijeta. Wi-Fi kao bežična tehnologija je postao sveprisutan u svakodnevnom životu da se uzima zdravo za gotovo. Wi-Fi je postojana mreža koja povezuje sve oko nas. Danas svi veći gradovi imaju besplatan pristup Internetu njegovim građanima i posjetiteljima. No ono što je bitno je brzina koju pruža mreža koju besplatna mreža nudi i to se danas pretvorilo u natjecanje između gradova. Vladajući ljudi natječu se kako i na koji način omogućiti građanima pouzdan i besplatan internet. Svima je od velikog interesa i koristi privući poslovne subjekte i stanovnike te im pružiti isplativ pristup informacijama[15].

5.1. Wi-Fi 6 (802.11ax)

IEEE od tekuće godine uvodi potpuno novi standard koji uvelike nadmašuje sve prijašnje standarde. Taj novi standard naziva se 802.11ax. Ovaj standard dizajniran je isključivo za javna okruženja visoke gustoće gdje se uvijek nalazi izrazito velik broj ljudi poput vlakova, stadiona ili zračnih luka, ali će ovaj standard biti vrlo koristan kada je u pitanju Internet stvari (eng. IoT – Internet of Things) te kod tvrtki koje zahtjevaju korištenje aplikacija s velikom potrebom korištenja mreže kao što su npr. videokonferencije. 802.11ax standard je također dizajniran za stanično iskrcavanje podataka (eng. cellular data offloading). Naime, to bi značilo da mobilne mreže „iskrcavaju“ svoj bežični promet te na taj način pojačavaju Wi-Fi mrežu u slučaju kada je prijem lokalnih stanica slaba.

Temeljni problem kod Wi-Fi mreža je taj da se propusnost dijeli između uređaja krajnjih točaka, točke pristupa mogu imati preklapajuća područja pokrivenosti, posebno u gustim sredinama, a krajnji se korisnici mogu kretati između raznih točaka pristupa. Trenutno rješenje, temeljeno na tehnologiji starih zajedničkih Ethernet dana nazvano Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), zahtijeva krajnje točke za slušanje

[15] GovInsider (2019.), *The Future of WiFi is here. It will transform cities forever*, GovInsider. Dostupno na: https://govinsider.asia/connected-gov/the-future-of-wifi-is-here-it-will-transform-cities-forever/ [15. srpnja 2019.]

potpuno jasnog signala prije prijenosa. U slučaju smetnji, zagušenja ili sudara krajnja točka prelazi u back-off postupak, čeka da sve bude „čisto“ te onda prenosi signal.

Na prepunim stadionima, prometnim zračnim lukama ili prepunom vlaku sa stotinama, pa čak i tisućama ljudi, krajnji korisnici pokušavaju u isto vrijeme npr. emitirati videozapise te sustav na taj način gubi učinkovitost i performanse. Dobra vijest kod 802.11ax standarda da on nudi poboljšanje performansi, proširenje pokrivenosti i duže trajanje baterije. Ovaj standard može isporučiti jedan tok podataka (stream) na 3.5 Gbps, te s novom tehnologijom multipleksiranja koja je posuđena iz svijeta LTE mobilne mreže, može isporučiti četiri istovremena stream-a na jednu krajnju točku za ukupnu teoretsku propusnost od čak 14 Gbps.

Standard 802.11ax uzima razne dobro razumljive bežične tehnologije i kombinira ih u jednu tako da postiže značajan napredak u odnosu na prethodne standarde, ali ipak zadržava kompatibilnost sa 802.11ac i 802.11n standardima. Standard 802.11ax omogućuje gotovo 40-postotno povećanje čiste propusnosti zahvaljujući QAM (quadrature amplitude modulation) modulaciji višeg reda koja omogućuje prijenos više podataka po paketu. Također se postiže učinkovitije korištenje spektra. Na primjer, 802.11ax stvara šire kanale i dijeli te kanale na uže podkanale. Time se povećava ukupni broj dostupnih kanala, što krajnjim točkama olakšava pronalaženje jasne putanje do točke pristupa. Kada je riječ o preuzimanju s točke pristupa do krajnjeg korisnika, rani Wi-Fi standardi dopuštali su samo jedan prijenos po točki pristupa. Wave 2 verzija 802.11ac standarda počela je koristiti Multi-User - Multi-Input Multi-Output (MU-MIMO), što je omogućilo točkama pristupa da šalju do četiri toka istovremeno. Standard 802.11ax omogućuje osam istovremenih stream-ova i koristi eksplicitnu tehnologiju oblikovanja snopa kako bi preciznije usmjerio te stream-ove na antenu prijamnika. Nešto što je još važnije, 802.11ax standard slojevito se nadodaje na MU-MIMO sa LTE tehnologijom koja se naziva Orthogonal Frequency Division Multiple Access (OFDMA). Ta tehnologija omogućuje da se svaki MU-MIMO tok podijeli u četiri dodatna toka čime se povećava djelotvorna propusnost po korisniku za četiri puta. Kolumnist Network World časopisa Zeus Kerrevala objašnjava standard 802.11ax na način da je rani Wi-Fi bio kao dugi red klijenata koje čekaju jednog blagajnika u banci. MU-MIMO je označavao četiri blagajnika

koji mogu poslužiti 4 reda klijenata, dok je OFDMA značio da svaki blagajnik može istovremeno poslužiti četiri klijenta.

U usporedbi sa standardnom 802.11ac koji radi na rasponu od 5GHz, standard 802.11ax radi na rasponima od 2,4GHz i do 5GHz i na taj način stvara više dostupnih kanala. Na primjer, rani čipseti podržavaju ukupno 12 kanala, osam u 5GHz i četiri u rasponu od 2,4GHz. Sa 802.11ac, MU-MIMO je ograničen samo na downlink prijenos. 802.11ax stvara full-duplex (komunikacija u oba smjera) MU-MIMO tako da sa downlink MU-MIMO točka pristupa može istovremeno prenositi signale na više prijamnika, a sa uplink MU-MIMO krajnja točka (korisnik) može istovremeno primati signale od više odašiljača. Standard 802.11ax podržava do osam MU-MIMO prijenosa odjednom, četiri više od koliko je podržavao standard 802.11ac. Poput nekih drugih tehnologija, OFDMA je novina kod 802.11ax standarda te uvodi nove funkcionalnosti kao što su slučajni pristup na temelju okidača, dinamička fragmentacija i ponovna upotreba prostorne frekvencije, sve s ciljem kako bi se povećala učinkovitost.

Konačno, standard 802.11ax uvodi tehnologiju zvanu „target wake time“ (ciljano vrijeme buđenja). Ta tehnologija koristi se za poboljšanje učinkovitosti buđenja i spavanja na pametnim telefonima te drugim mobilnim uređajima. Očekuje se da će ova tehnologija znantno produžiti vijek trajanja baterije mobilnih uređaja[16].

5.2. Internet of Things (Internet stvari)

Kroz posljednjih nekoliko godina, vidjeli smo da se Wi-Fi koristi samo od nekolicine velikih, glomaznih računala s mnoštvom tankih, lakih prijenosnih računala, tableta i ponajviše pametnih telefona. Također, vidimo da se i razni drugi uređaji (kao što su pisači, klimatizacijski uređaji i drugi) povezuju na Wi-Fi mrežu kako bi poboljšali lakoću rada, odmora, učenja i igranja. U sljedećih nekoliko godina, bilo bi potrebno obratiti pažnju na „Internet stvari“ (eng. Internet of Things – IoT) – jedne velike mreže u suštini bilo kojeg proizvoda koji je moguće zamisliti prožete bežičnom povezanošću. Trenutno, na tržište

[16] Weinberg, N. (2018.), *What is 802.11ax Wi-Fi, and what will it mean for 802.11ac,* Network World. Dostupno na: https://www.networkworld.com/article/3258807/what-is-802-11ax-wi-fi-and-what-will-it-mean-for-802-11ac.html [16. srpnja 2019.]

dolaze razni uređaji sa takvom mogućnošću od hladnjaka, zamrzivača koji mogu sami preurediti raspored namirnica ili kuhala koja mogu zagrijati vodu na zahtjev osobe koja upravlja njime. Do sad je već viđeno puno takvih uređaja koji su postali stvarnost pomoću velike razine korištenja pametne tehnologije i doista pametnih domova koji postaju komercijalno dostupni. Cijena će, kroz godine koje dolaze, postajati samo pristupačnija, pa je to područje koje ima velike izglede za uspijeh u slučaju da se želite odvažiti na takav pothvat i pokrenut takvo zanimanje[17].

6. BRZINE WI-FI-ja U SVIJETU

Brzine interneta u svijetu nisu jednako raspoređene pa tako imamo države sa odličnim brzinama javnih Wi-Fi mreža (obično su to dobro razvijene zemlje) i države sa izrazito malim brzinama koje ne zadovoljavaju normalan rad uređaja spojenih na neku javnu Wi-Fi mrežu. Kako svaka država ima svoju ekonomsku politiku, velik utjecaj ima i veza sa tehnologijom koja uvelike utječe kako ta država stoji u usporedbi sa nekim susjednim zemljama koje ju okružuju.

Prilikom navigacije u javnim Wi-Fi točkama pristupa, do brzog Interneta s internetskim telefonskim uslugama nije uvijek lako doći. Top 20 zemalja za javne Wi-Fi mreže su uglavnom smještene u Europi, pa su tako Litva i Hrvatska vodeće sa najvećim brzinama preuzimanja na javnim Wi-Fi mrežama. Tako na primjer u Litvi, javne Wi-Fi mreže u prosjeku nude otprilike 15.4 Mbps za preuzimanja te 14.17 Mbps za učitavanje (eng. upload). Hrvatska je druga na toj listi sa brzinom oko 14.05 Mbps pri preuzimanju te oko 11.21 Mbps kada je u pitanju upload.

U svijetu danas postoji približno 189 milijuna Wi-Fi pristupnih točaka što je rast od nevjerovatnih 888% koje je zabilježeno 2013. godine. S obzirom na to koliki je broj ljudi na jednu javnu pristupnu točku Wi-Fi mreže, u tom segmentu prednjači Francuska sa 2.8

[17] Redway Networks, (2018.), *The future of WiFi: 3 trends which could shape the future*, Redway Networks. Dostupno na: https://www.redwaynetworks.com/the-future-of-wifi/ [16. srpnja 2019.]

osoba po jednoj pristupnoj točki. Zadnja u tom segmentu je Kolumbija u kojoj se na jednu javnu Wi-Fi mrežu spaja čak 214,523.10 osoba što je ogroman broj te takva mreža nudi izrazit male brzine sa preuzimanje/učitavanje podataka.

Globalna prosječna brzina Wi-Fi mreža iznosi 6.1 Mbps što nije izrazito velika brzina kada se pogleda prosječna brzina nekih država. Tako npr. Južna Koreja ima najveću prosječnu brzinu (uključujući stambeni i komercijalni pristup internetu) koja iznosi čak 27 Mbps. Druga na ljestvici prosječne brzine Wi-Fi mreže po državi je Norveška sa 20 Mbps, a treći je Hong Kong sa malo manje od 20 Mbps. Kada su u pitanju najsporije prosječne brzine prva na ljestvici je Nigerija sa 3 Mbps, druga je Bolivija sa 2 Mbps koliko ima i treća država na ljestvici, Namibija. Tu je, dakle, vrlo očita razlika u brzinama s obzirom koliko su razvijene države gledajući njihovu ekonomsku situaciju. Zanimljiv podatak je taj da Južna Koreja ima približno duplo veću brzinu od one koju imaju Sjedinjene Američke Države. Razlozi tome su izrazita konkurencija među širokopojasnim operatorima, relativan sustav otvorenih (javnih) Wi-Fi mreža u kojoj tvrtke dijele infrastrukturu, gusta populacija koja smanjuje potrebu za ožičenjem te proaktivni vladin tehnološki plan donese 1990-ih godina.

Kada je riječ o mobilnoj povezanosti po državi, tu prednjači Ujedinjeno Kraljevstvo sa brzinama spajanja blizu 23.1 Mbps. Druga je Belgija sa 21.1 Mbps, a treći je Cipar sa prosječnom brzinom mobilne mreže od 20 Mbps. Države sa najsporijom mobilnom mrežom su Panama sa brzinom od 2.9 Mbps te Argentina i Ekvador sa brzinama od 2.8 Mbps. U 2018. godini, četiri države su zabilježile najveće rastuću brzinu interneta u posljednjih 10 godina. To su Kenija (sa rastom od 297%), Indonezija (148%), Egipat (110%) te Katar (101%)[18].

[18] Hazanchuk, A. (2018.), *Best and Worst Countries for Wi-Fi Access*, Ooma. Dostupno na: https://www.ooma.com/blog/best-worst-wifi-countries/ [23. srpnja 2019.]

7. ZAKLJUČAK

Wi-Fi kao vrsta bežičnog spajanja na mrežu je trenutno u svom najboljem stadiju. Izričito je jednostavan za korištenje i kroz mnoge prednosti, od kojih su neke učinkovitost, fleksibilnost, isplativost te pristupačnost, uvelike olakšava rad ljudima kojima u nekim nužnim situacijama može omogućiti Internet i pregled čega god požele. S obzirom da je danas sigurnost, u bilo kojem obliku, danas svim ljudima prioritet, isto je i sa Wi-Fi-om. Naime, najveća mana Wi-Fi mreža je sigurnost te se velikim naporima taj problem pokušava riješiti kroz razne sigurnosne propuste. Sve je počelo sa WEP protokolom, koji je trebao imati približno jednaku zaštitu kao i žičane mreže. Nakon što je otkriveno da WEP ima izrazito puno nedostataka i sigurnosnih problem koje je, čak i u to vrijeme, bilo lako zaobići, predstavljen je WPA protokol koji kroz nekoliko godina dobija i svog nasljednika a to je WPA2. Danas, WPA2 je najrašireniji i najčešće korišteni sigurnosni protokol koji je vrlo teško probiti.

Wi-Fi izrazito napreduje pa tako dobijamo mreže sa po nekoliko stotina Mbps što je unazad 10 i više godina bilo nezamislivo, pa čak i za žičano povezivanje. U najavi su razni standardi kako bi se povećala kako sigurnost, tako i sama brzina spajanja. Tako se i uvelike razvija Internet Stvari kojim bi se omogućilo spajanje bilo kojih uređaja na mrežu te lakše upravljanje njima.

S druge strane, osim sigurnosti, Wi-Fi kao bežični sustav ima još nedostataka. Mali domet signala i nemogućnost stopostotne zaštite su najveći problemi koji trenutno opsjedaju Wi-Fi. Sa sigurnošću se može reći da je Wi-Fi promijenio svijet i omogućio mnogim ljudima pristup internetu bez da moraju nužno biti povezani žicom, kao i što će se nastaviti njegov razvoj dalje u budućnosti.

POPIS IZVORA

1. Radovan, M. (2010). *Računalne mreže (1),* Rijeka. Digital point tiskara
2. Arun (2013). *What is Wi-Fi* [online], Scribd. Dostupno na: https://www.scribd.com/document/192846073/Wifi [03. srpnja 2019.]
3. Fitzpatrick, J. (2017). *The Difference between WEP, WPA and WPA2 Wi-Fi Passwords* [online], How-To-Geek. Dostupno na: https://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/ [09. srpnja 2019.]
4. GovInsider (2019). *The future of WiFi is here. It will transform cities forever* [online], GovInsider. Dostupno na: https://govinsider.asia/connected-gov/the-future-of-wifi-is-here-it-will-transform-cities-forever/ [15. srpnja 2019.]
5. Hazanchuk, A. (2018). *Best and Worst Countries for Wi-Fi Access* [online], Ooma. Dostupno na: https://www.ooma.com/blog/best-worst-wifi-countries/ [23. srpnja 2019.]
6. Joseph, C., *What does a Wi.Fi repeater do?* [online], Small Business – Chron.com. Dostupno na: https://smallbusiness.chron.com/wifi-repeater-do-31941.html [09. srpnja 2019.]
7. Karan, T., Aggarwal, A., Masih D., (2018). *Wi-Fi Technology* [online], Scribd. Dostupno na: https://www.scribd.com/document/373130860/WiFi-Technology-Bss [03. srpnja 2019.]
8. Krishnasamy, T. (2017). *What are the advantages and disadvantages of WiFi?* [online], Quora. Dostupno na: https://www.quora.com/What-are-the-advantages-and-disadvantages-of-WiFi [03. srpnja 2019.]
9. Mitchell, B. (2019). *What is a modem in Computer Networking?* [online], Lifewire. Dostupno na: https://www.lifewire.com/what-is-a-modem-817861 [16. srpnja 2019.]
10. Mitchell, B. (2019). *The range of typical Wi-Fi Network* [online], Lifewire. Dostupno na: https://www.lifewire.com/range-of-typical-wifi-network-816564 [04. srpnja 2019.]

11. Netspot. *Wi-Fi encryption and security* [online], Netspotapp. Dostupno na: https://www.netspotapp.com/wifi-encryption-and-security.html [09. srpnja 2019.]
12. Pinola, M. (2019). *How To Set up Your Home Wi-Fi Network* [online], Lifewire. Dostupno na: https://www.lifewire.com/how-to-set-up-your-home-wi-fi-network-2378223 [15. srpnja 2019.]
13. Redway Networks, (2018). *The future of WiFi: 3 trends which could shape the future* [online], Redway Networks. Dostupno na: https://www.redwaynetworks.com/the-future-of-wifi/ [16. srpnja 2019.]
14. Solver One Blog. *The Pros and Cons of Wi-Fi* [online], Washington, D.C. Dostupno na: https://www.solvereone.com/pages/the-pros-and-cons-of-wi-fi/ [02. srpnja 2019.]
15. Spahić, A. (2011). *Bežične Wi-Fi Računarske mreže i sigurnost Wi-Fi mreža*, seminarski rad. Zenica : Pedagoški Fakultet [24. srpnja 2019.]
16. Weinberg, N. (2018). *What is 802.11ax Wi-Fi, and what will it mean for 802.11ac* [online], Network World. Dostupno na: https://www.networkworld.com/article/3258807/what-is-802-11ax-wi-fi-and-what-will-it-mean-for-802-11ac.html [16. srpnja 2019.]

POPIS SLIKA

SAŽETAK

U današnje vrijeme, Wi-Fi je postao neizostavan dio ugostiteljskih obrta, hotela, restorana, zračnih luka i raznih drugih mjesta s obzirom da Internet danas pokreće svijet. Tema mog završnog rada je upravo bila Wi-Fi kao vrsta bežičnog povezivanja. Wi-Fi nudi fleksibilnost, poboljšanje učinkovitosti rada te je uvelike isplativ jer troškovi opreme i postavljanja same Wi-Fi mreže nisu veliki. No kako se Wi-Fi razvijao, tako su se razvijali načini probijanja sigurnosti tog bežičnog načina povezivanja pa je tako najveća mana Wi-Fi-ja njegova sigurnost. Svakoj osobi koja koristi neku Wi-Fi mrežu stavlja se naglasak na sigurnost, te se baš iz tog razloga uvelike radi na tome kako bi se povećala sigurnost i očuvanje podataka korisnika Wi-Fi mreže.

Ključne riječi: Wi-Fi, sigurnost, bežično povezivanje

SUMMARY

Nowadays, Wi-Fi has become an indispensable part of the hospitality industry, hotels, restaurants, airports and various other places as the Internet powers the world. The theme of my final thesis is just Wi-Fi as a type of wireless connectivity. Wi-Fi offers flexibility, improved work efficinecy and is very cost effective because the cost of equipment and setup of the Wi-Fi network itself is not expensive. But as Wi-Fi evolved, so did the ways of breaking through the security of this type of wireless connectivity, and so the biggest drawback is its security. Every person using a Wi-Fi network is stressed about security, and for this very reason much work is being done to increase the security and information preservation of Wi-Fi network users.

Keywords: Wi-Fi, security, wireless connectivity